FIG. 1

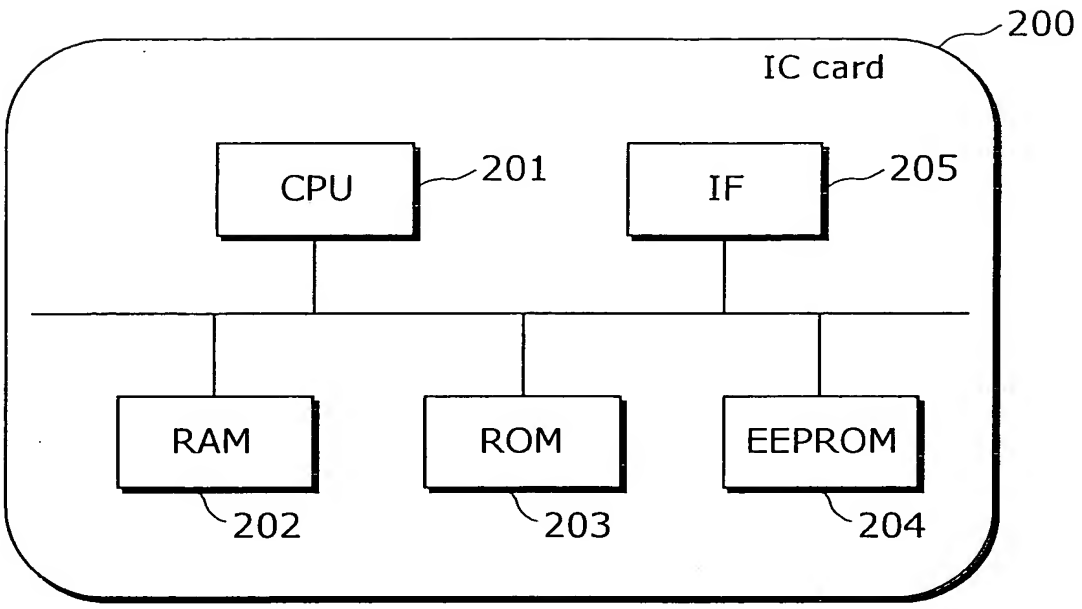
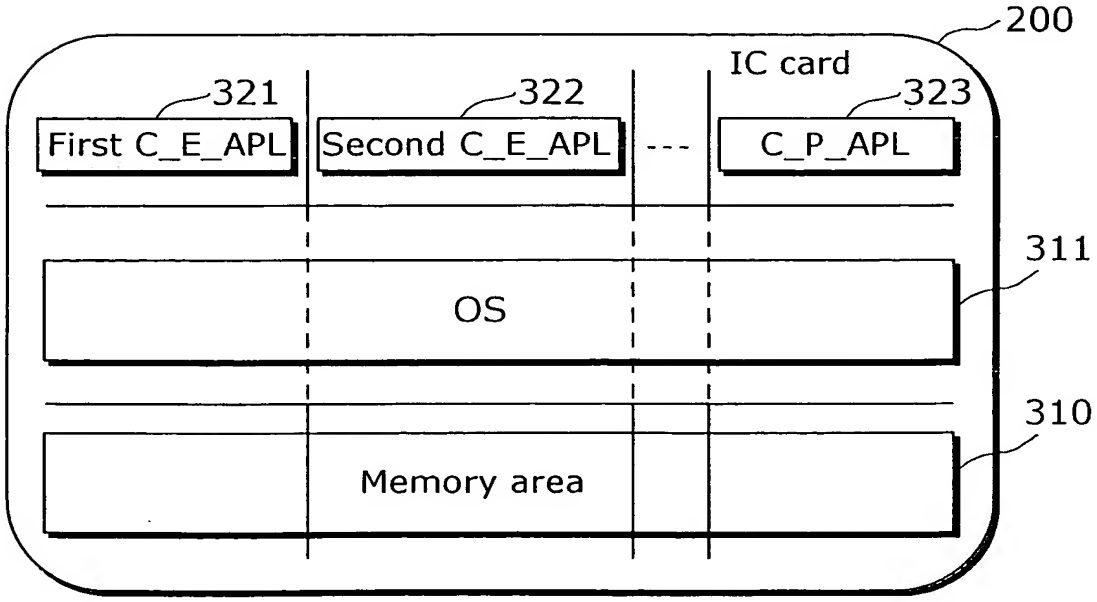

200
IC card
CPU
201
IF
205
RAM
202
ROM
203
EEPROM
204

FIG. 2


200
IC card
321
First C_E_APL
322
Second C_E_APL

323
C_P_APL
311
OS
310
Memory area

FIG. 3

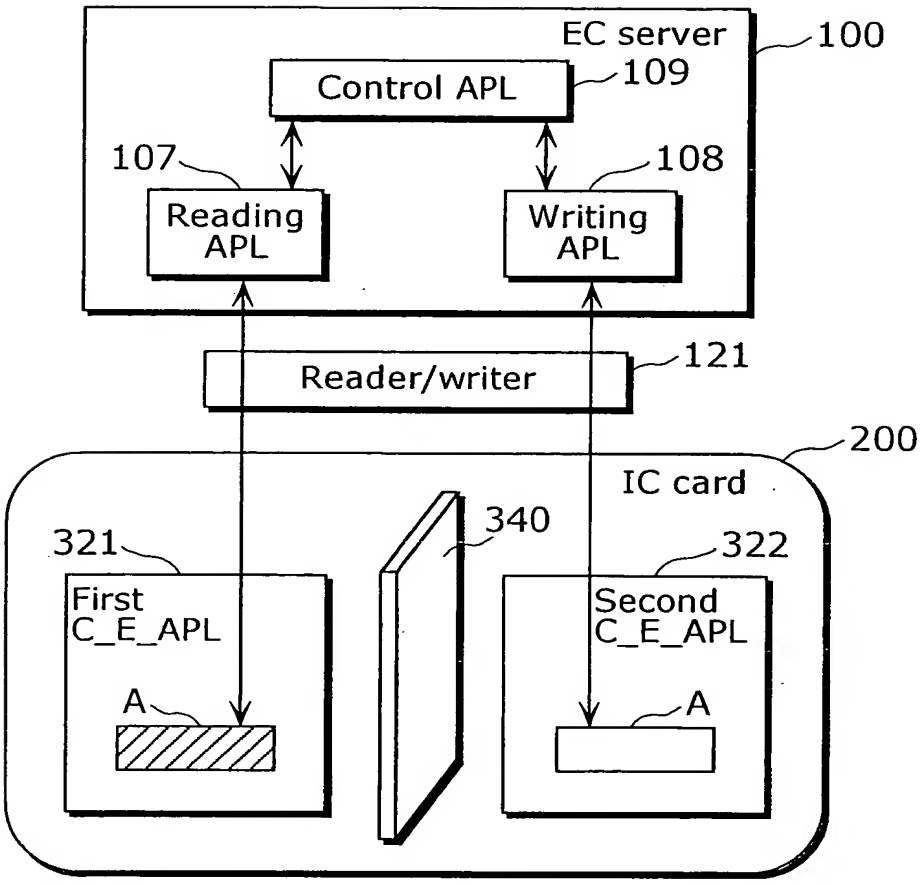

EC server
100
Control APL
109
107
108
Reading APL
Writing APL
Reader/writer
121
200
IC card
340
321
322
First C_E_APL
Second C_E_APL
A
A

FIG. 4

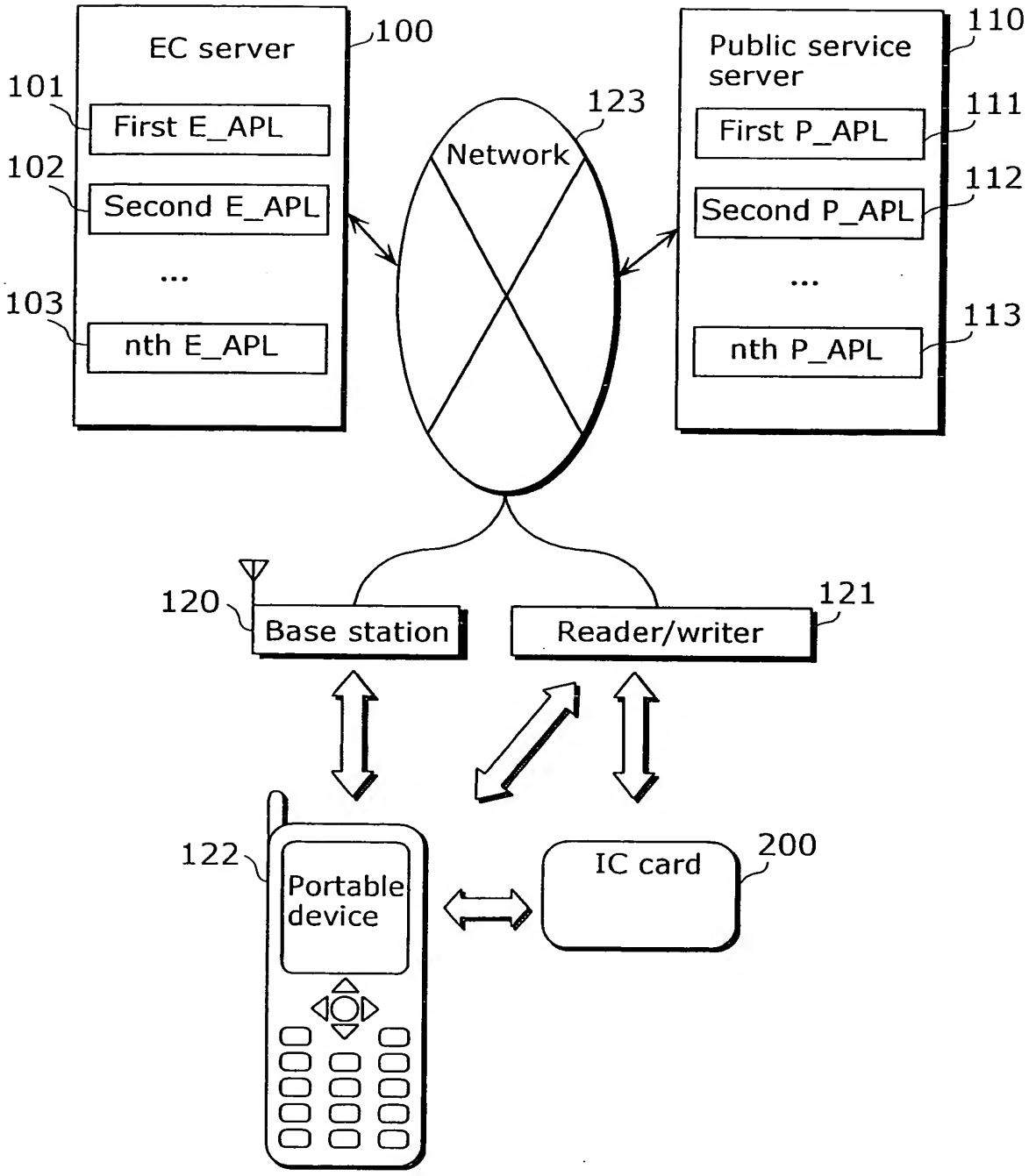

EC server
100
101
First E_APL
102
Second E_APL
...
103
nth E_APL
Network
123
Public service server
110
First P_APL
111
Second P_APL
112
...
nth P_APL
113
120
Base station
Reader/writer
121
122
Portable device
IC card
200

FIG. 5

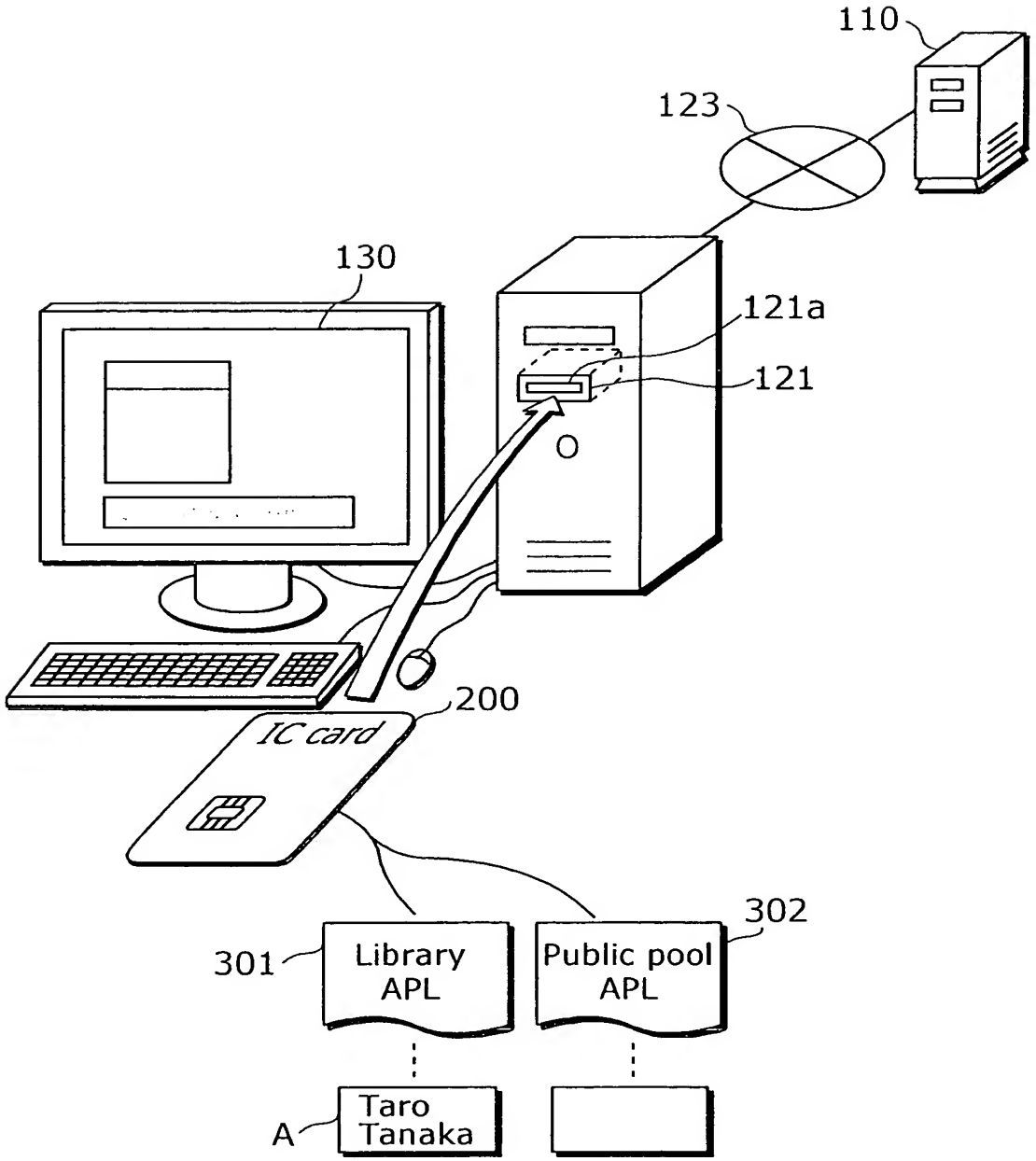

110
123
130
121a
121
200
IC card
302
301
Library APL
Public pool APL
A
Taro Tanaka

FIG. 6

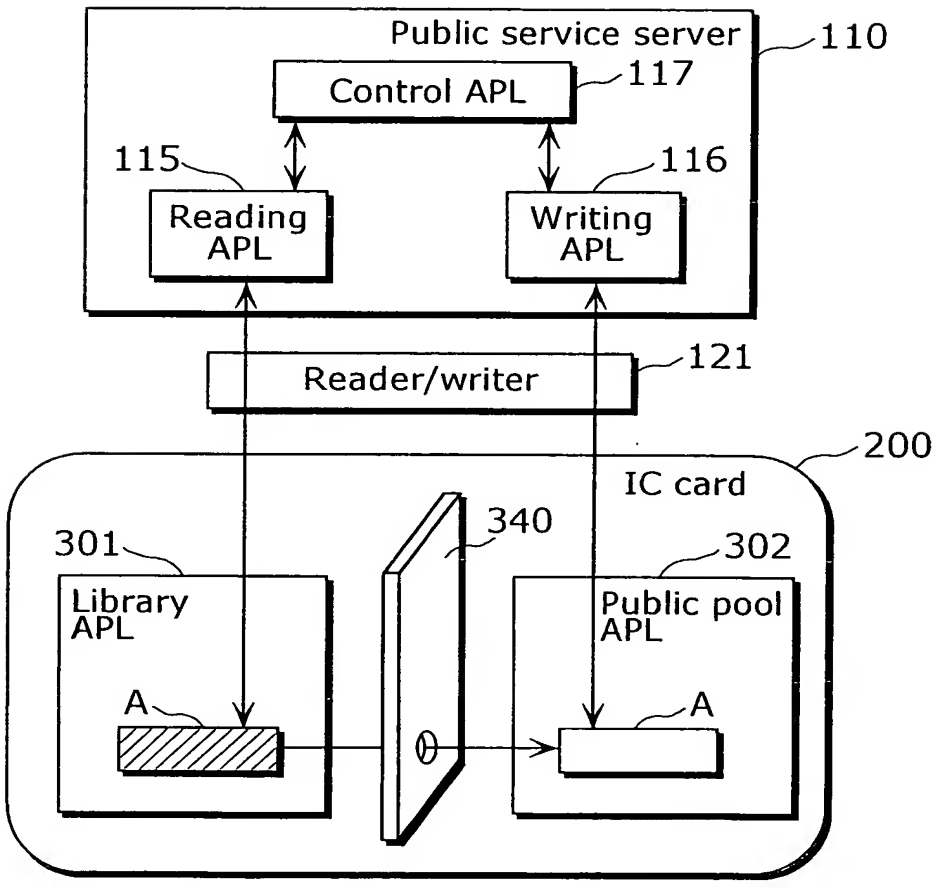

Public service server
110
Control APL
117
115
116
Reading APL
Writing APL
Reader/writer
121
200
IC card
340
301
302
Library APL
Public pool APL
A
A

FIG. 7

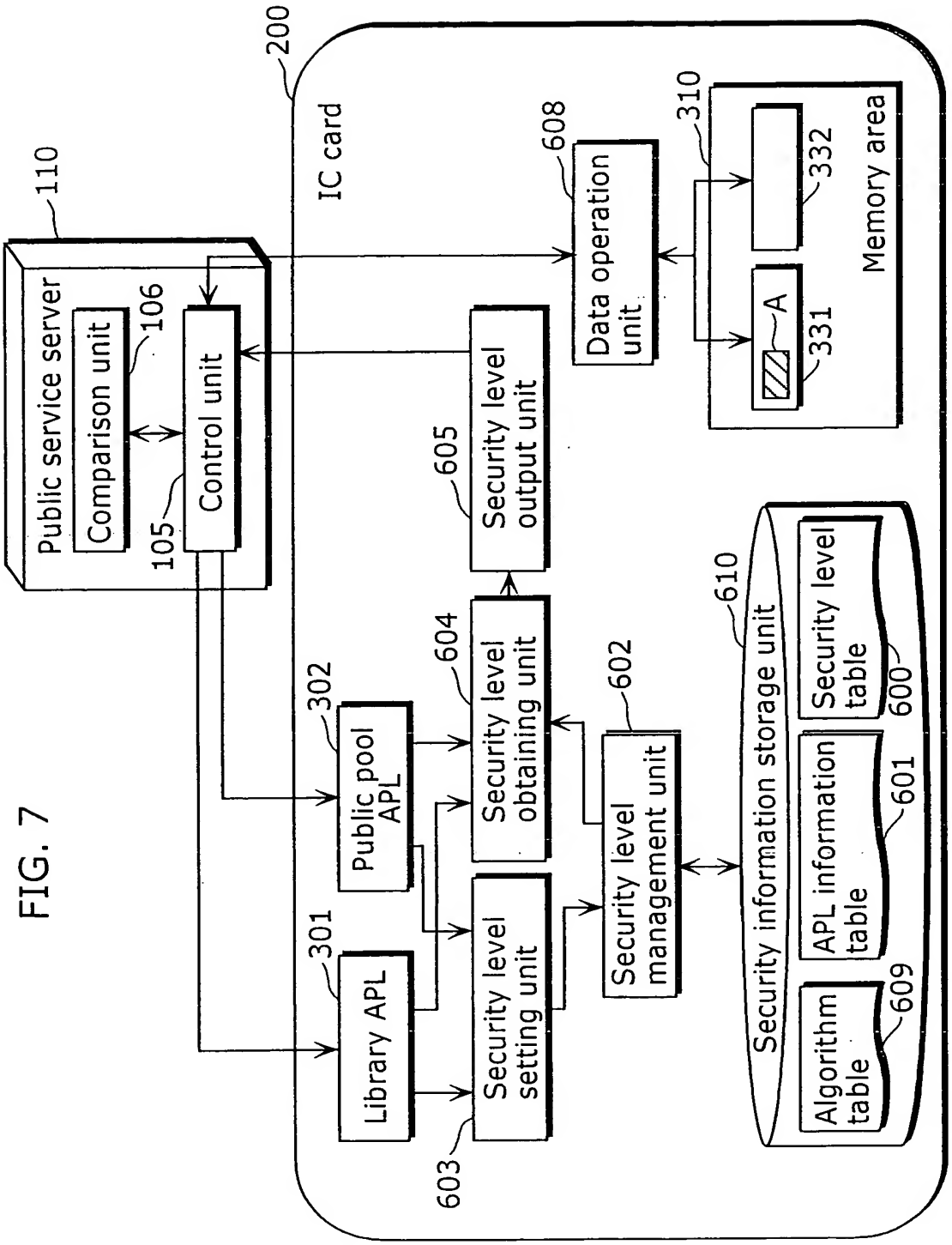

110
Public service server
Comparison unit
106
Control unit
105
200
IC card
608
Data operation unit
310
332
A
331
Memory area
605
Security level output unit
604
Security level obtaining unit
602
Security level management unit
610
Security information storage unit
Security level table
600
APL information table
601
Algorithm table
609
302
Public pool APL
301
Library APL
603
Security level setting unit

FIG. 8

600

Security level table		
Level	Value	Encryption algorithm
Strong	03h	Triple-DES
Medium	02h	DES
Weak	01h	AES
None	00h	No encryption

FIG. 9

609

Algorithm table	
Number	Encryption algorithm
0	Triple-DES
1	DES
2	AES
3	No encryption

FIG. 10

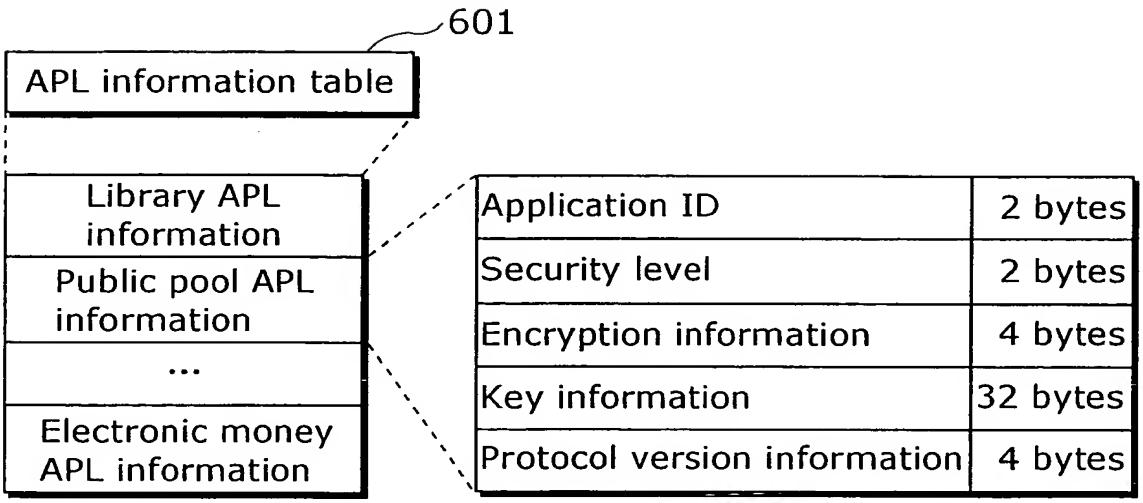

601
APL information table
Library APL information
Public pool APL information
...
Electronic money APL information
Application ID
2 bytes
Security level
2 bytes
Encryption information
4 bytes
Key information
32 bytes
Protocol version information
4 bytes

FIG. 11

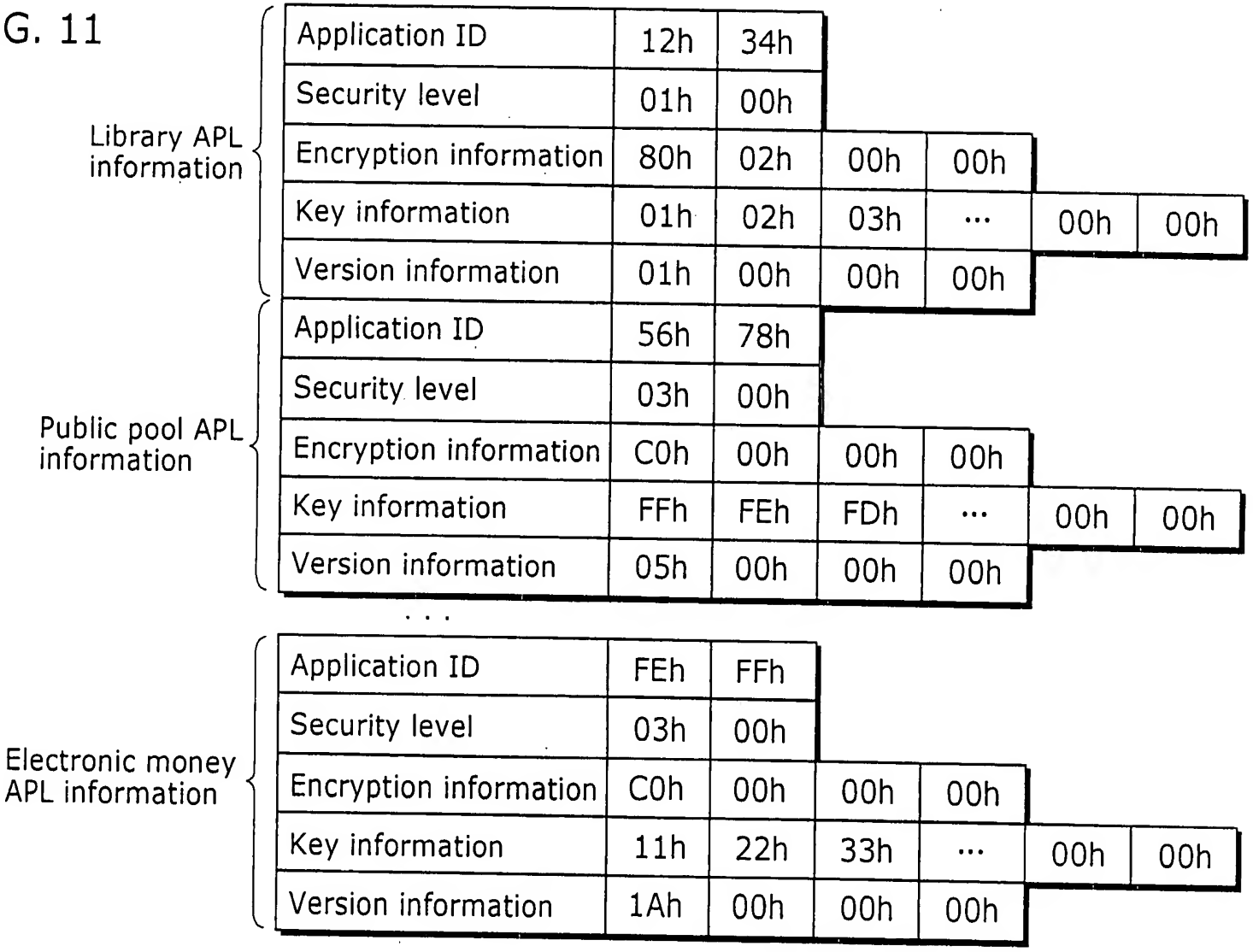

Library APL information
Application ID 12h 34h
Security level 01h 00h
Encryption information 80h 02h 00h 00h
Key information 01h 02h 03h ··· 00h 00h
Version information 01h 00h 00h 00h
Public pool APL information
Application ID 56h 78h
Security level 03h 00h
Encryption information C0h 00h 00h 00h
Key information FFh FEh FDh ··· 00h 00h
Version information 05h 00h 00h 00h
Electronic money APL information
Application ID FEh FFh
Security level 03h 00h
Encryption information C0h 00h 00h 00h
Key information 11h 22h 33h ··· 00h 00h
Version information 1Ah 00h 00h 00h

FIG. 12

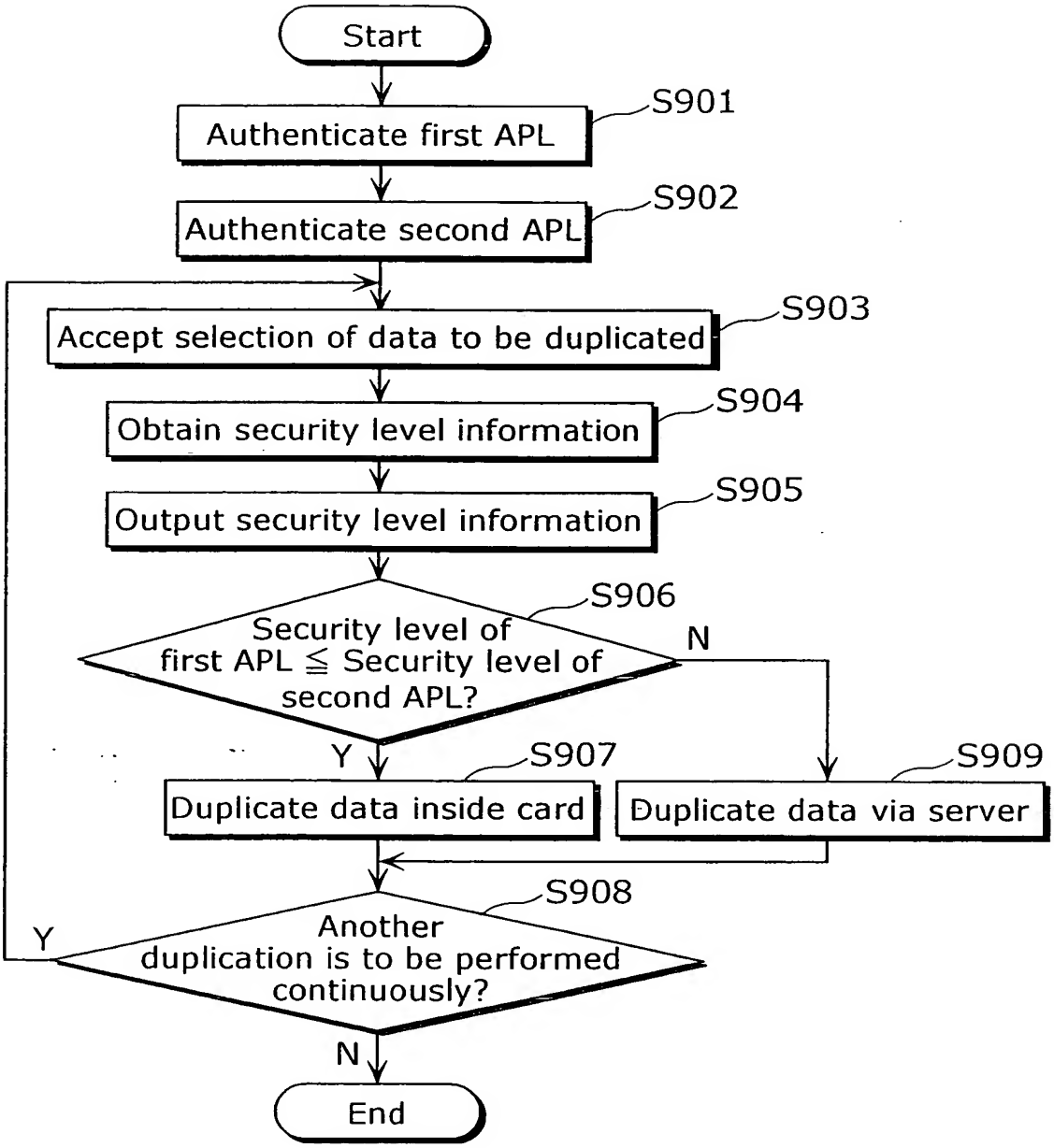

Start
Authenticate first APL
S901
Authenticate second APL
S902
Accept selection of data to be duplicated
S903
Obtain security level information
S904
Output security level information
S905
Security level of first APL ≦ Security level of second APL?
S906
N
Y
Duplicate data inside card
S907
Duplicate data via server
S909
Another duplication is to be performed continuously?
S908
Y
N
End

FIG. 13

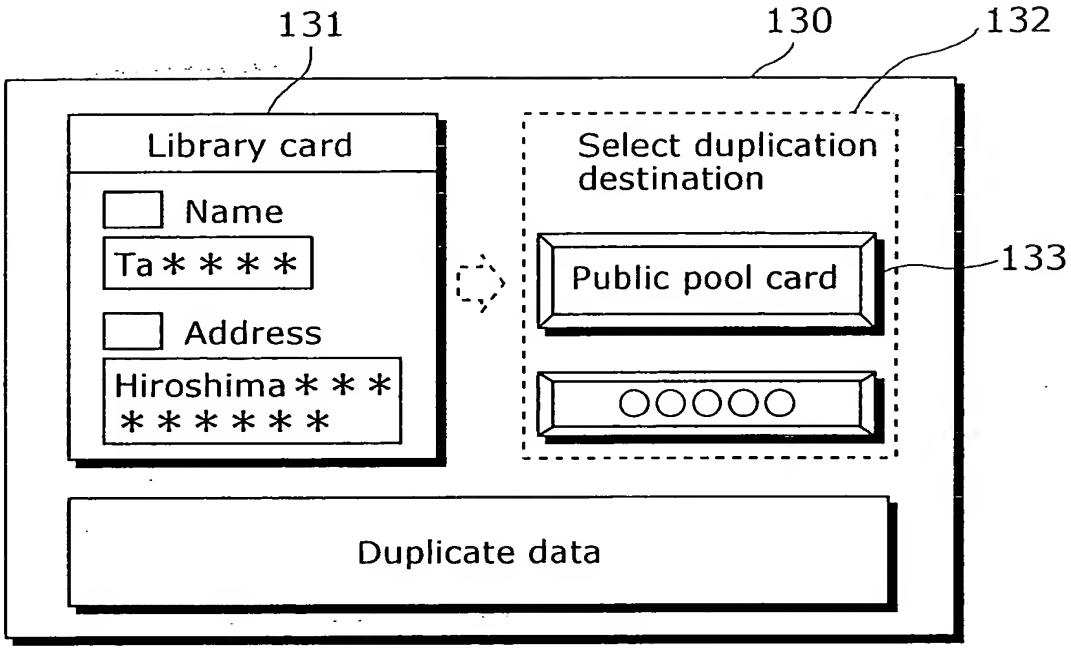

131
130
132
Library card
Name
Ta＊＊＊＊
Address
Hiroshima＊＊＊
＊＊＊＊＊＊
Select duplication destination
Public pool card
133
○○○○○
Duplicate data

FIG. 14

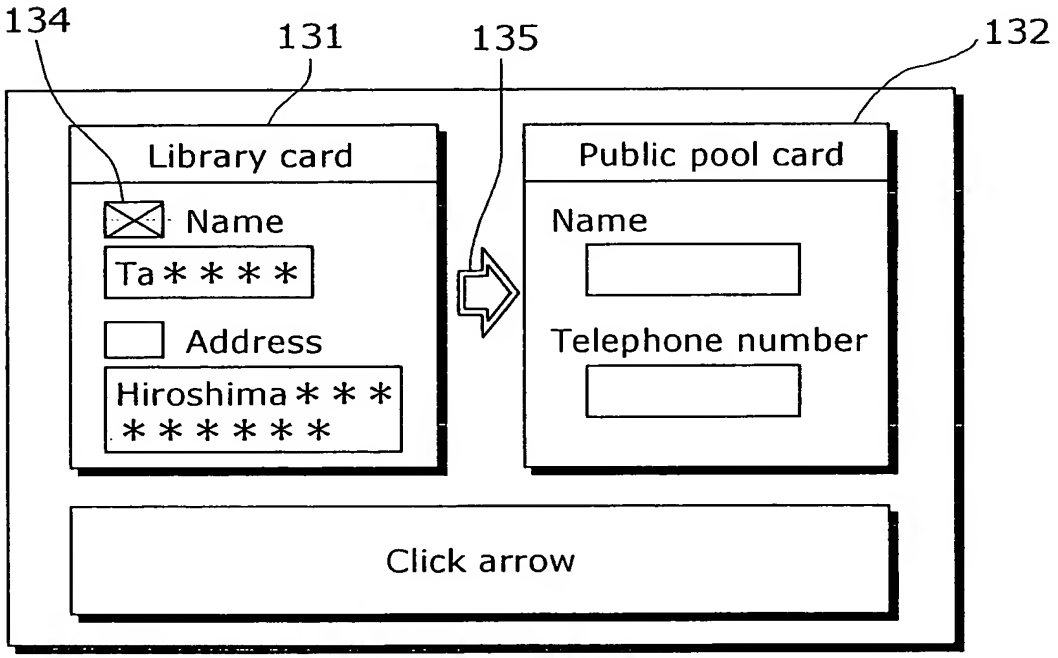

134
131
135
132
Library card
Name
Ta＊＊＊＊
Address
Hiroshima＊＊＊
＊＊＊＊＊＊
Public pool card
Name
Telephone number
Click arrow

FIG. 15

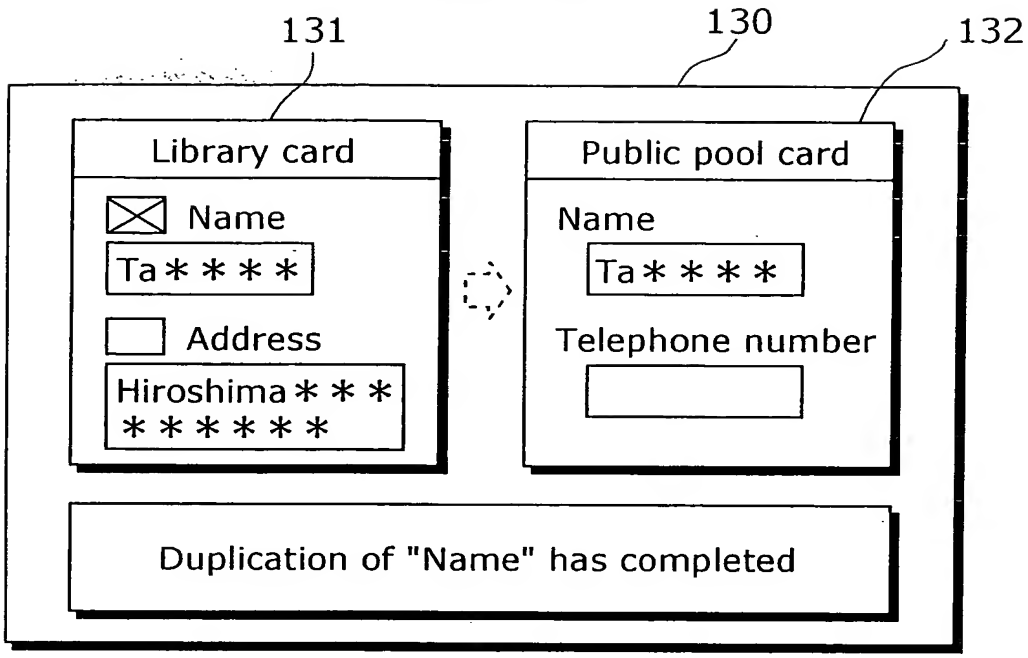

131
130
132
Library card
Name
Ta＊＊＊＊
Address
Hiroshima＊＊＊
＊＊＊＊＊＊
Public pool card
Name
Ta＊＊＊＊
Telephone number
Duplication of "Name" has completed

FIG. 16

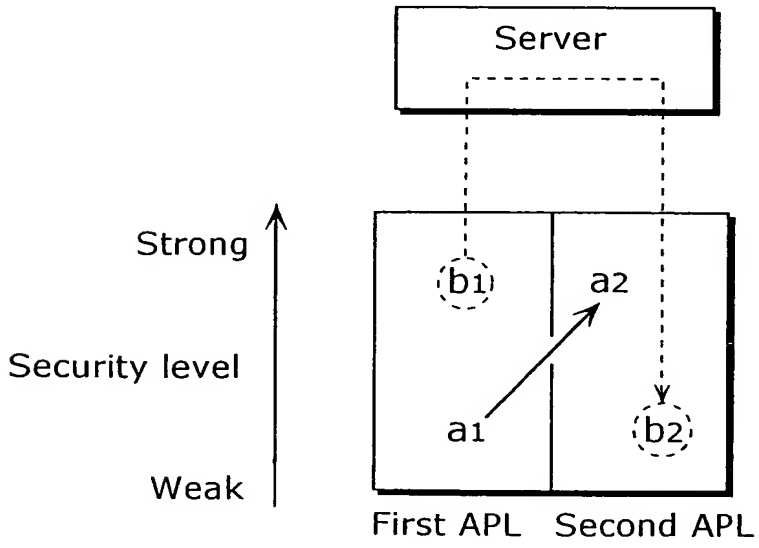

Server
Strong
Security level
Weak
b1
a2
a1
b2
First APL
Second APL

FIG. 17

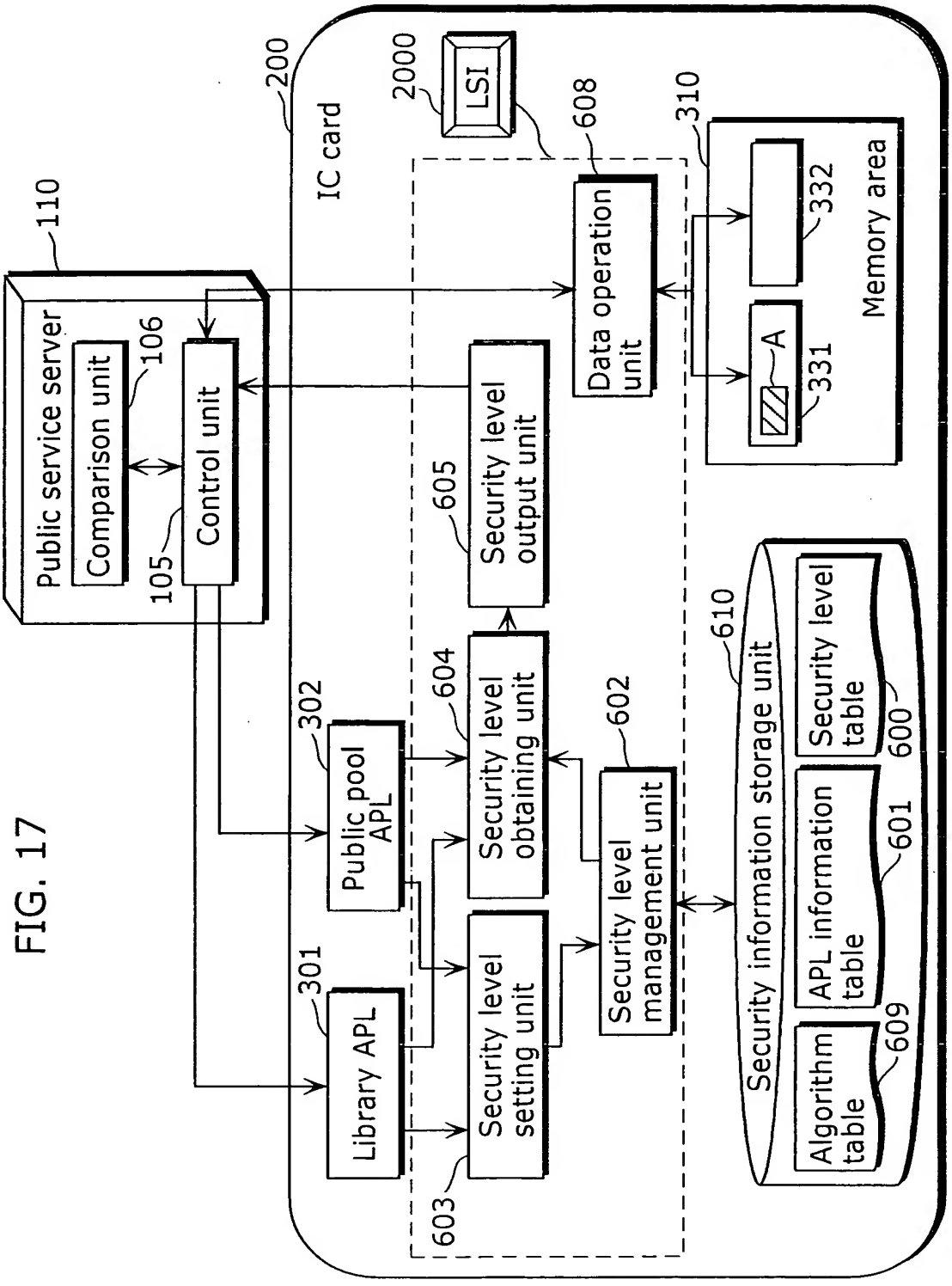

110
Public service server
Comparison unit
106
Control unit
105
200
IC card
2000
LSI
608
Data operation unit
310
Memory area
332
A
331
605
Security level output unit
604
Security level obtaining unit
602
Security level management unit
610
Security information storage unit
Security level table
600
APL information table
601
Algorithm table
609
302
Public pool APL
301
Library APL
Security level setting unit
603

FIG. 18

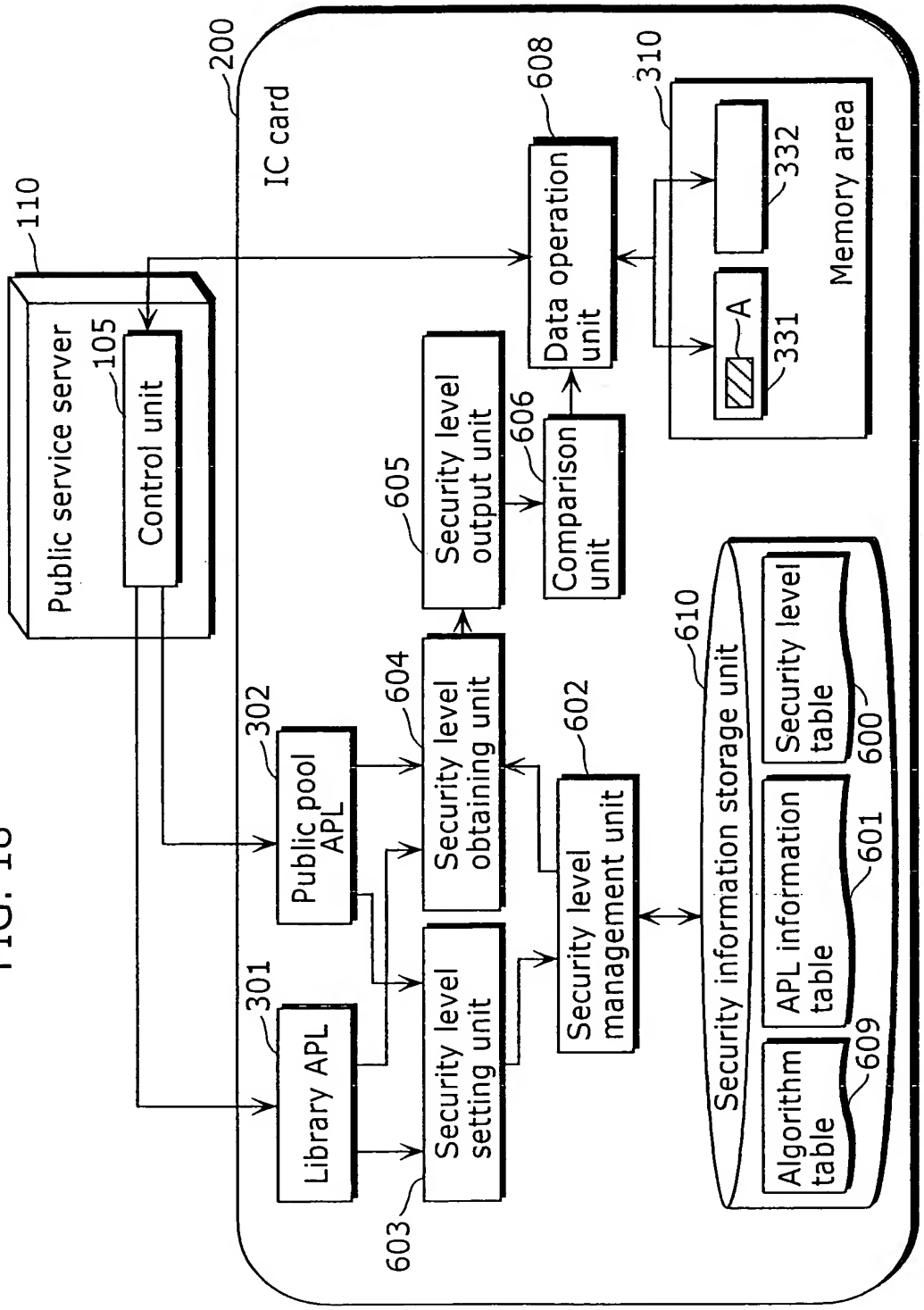

110
Public service server
105
Control unit
200
IC card
608
Data operation unit
310
Memory area
332
A
331
605
Security level output unit
606
Comparison unit
610
Security information storage unit
Security level table
600
APL information table
601
Algorithm table
609
302
Public pool APL
604
Security level obtaining unit
602
Security level management unit
301
Library APL
Security level setting unit
603

FIG. 19

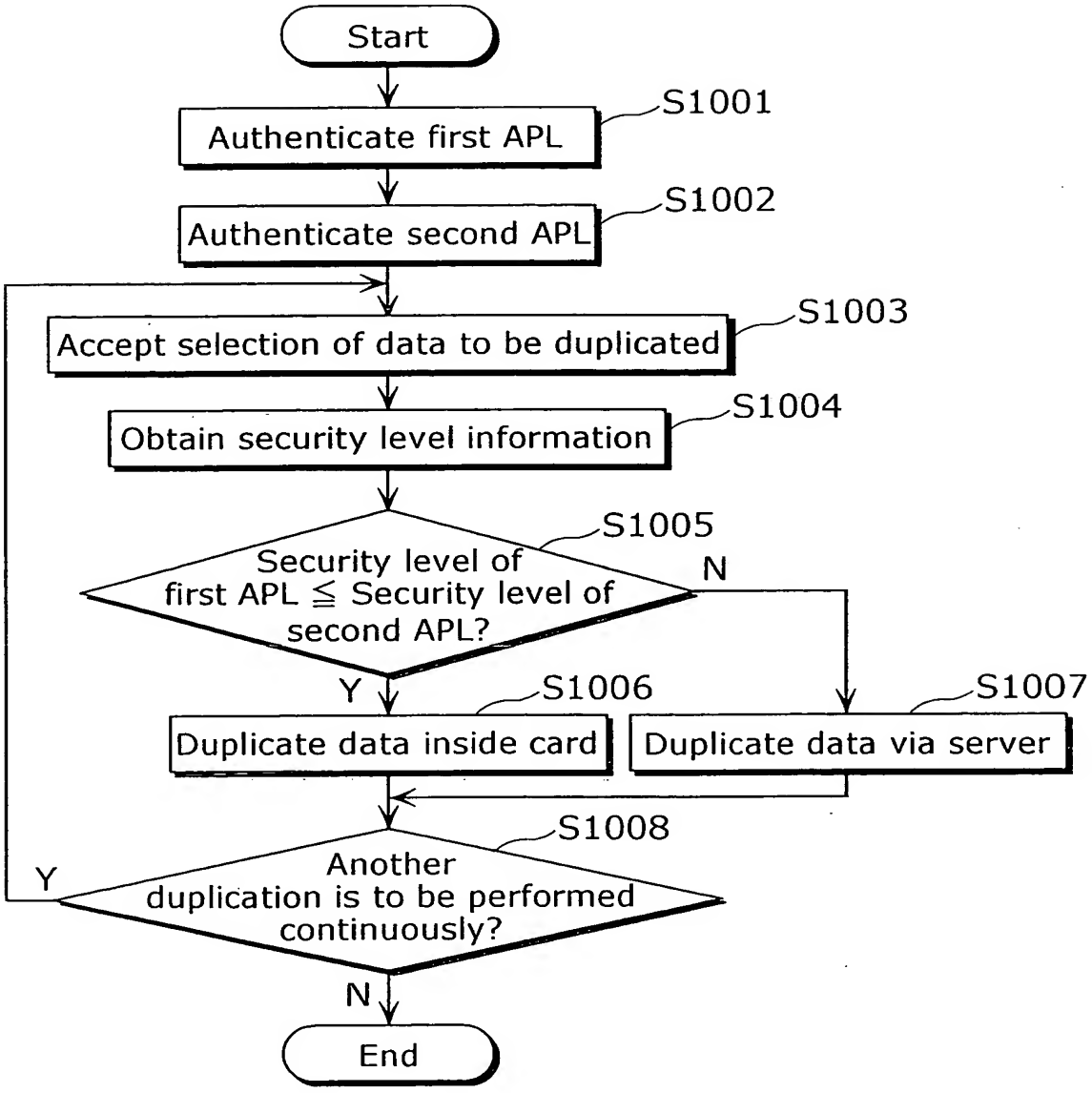

Start
Authenticate first APL
S1001
Authenticate second APL
S1002
Accept selection of data to be duplicated
S1003
Obtain security level information
S1004
Security level of first APL ≦ Security level of second APL?
S1005
N
Y
Duplicate data inside card
S1006
Duplicate data via server
S1007
Another duplication is to be performed continuously?
S1008
Y
N
End

FIG. 20

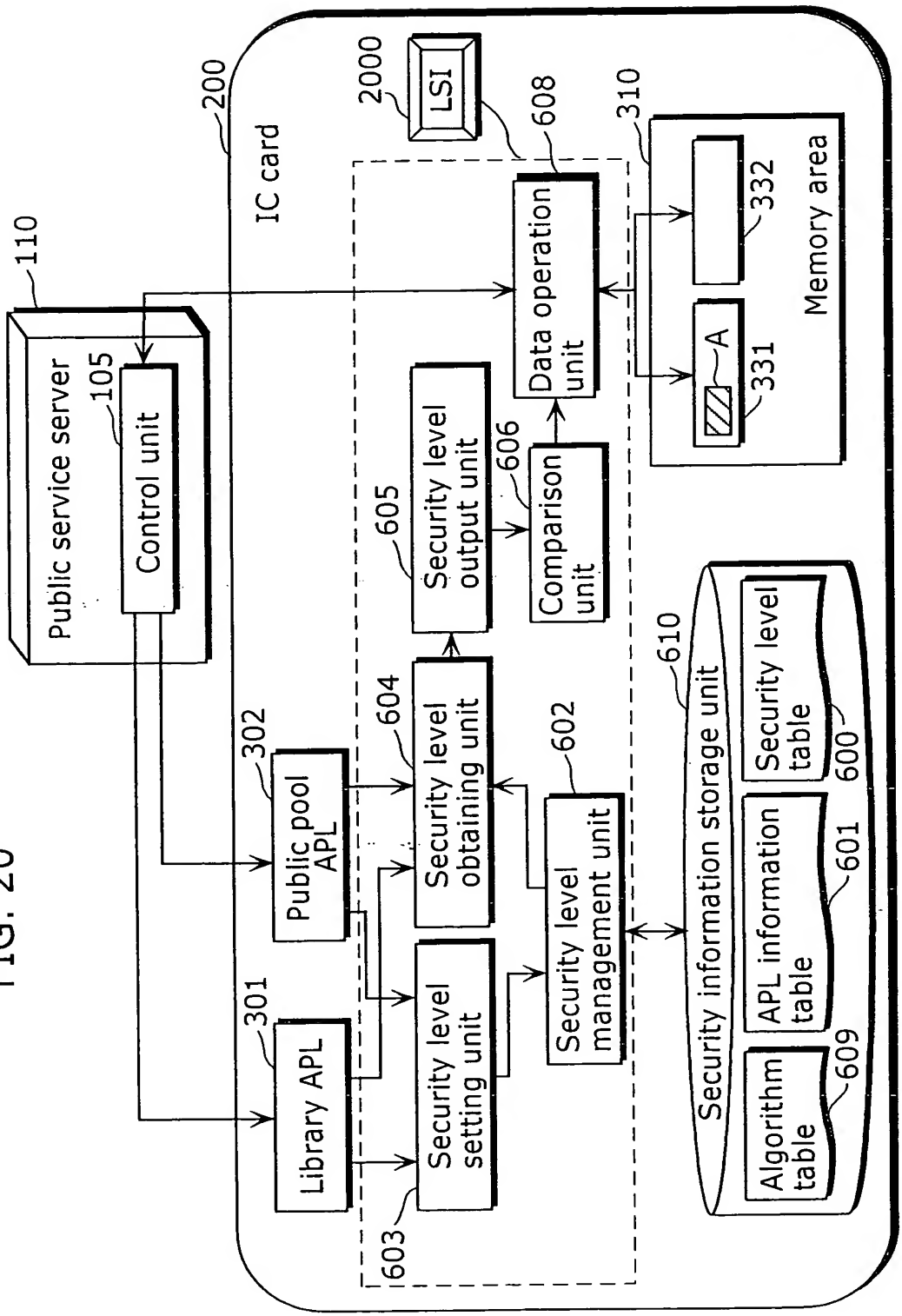

110
Public service server
105
Control unit
200
IC card
2000
LSI
608
Data operation unit
310
Memory area
332
A
331
605
Security level output unit
606
Comparison unit
610
Security information storage unit
Security level table
600
APL information table
601
Algorithm table
609
604
Security level obtaining unit
602
Security level management unit
302
Public pool APL
301
Library APL
Security level setting unit
603

FIG. 21

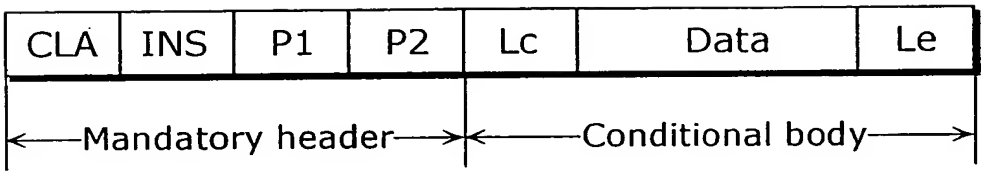


FIG. 22

Command name	SELECT	READ RECORD	INTERNAL AUTHENTICATE
CLA(1byte)	00h	00h	00h
INS(1byte)	A4h	B2	88h
P1(1byte)	XXh	Record Number	00h
P2(1byte)	00h	XXh	00h

FIG. 23

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	Select MF, DF and EF
0	0	0	0	0	0	0	1	Select child DF
0	0	0	0	0	0	1	0	Select EF under current DF
0	0	0	0	0	0	1	1	Select parent DF of current DF
0	0	0	0	0	1	0	0	Direct selection by DF name
0	0	0	0	1	0	0	0	Select from MF
0	0	0	0	1	0	0	1	Select from current DF
								Any other value: Not specified

FIG. 24

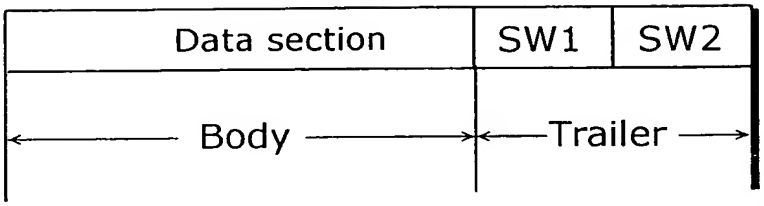


FIG. 25

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0					Common command
1	0	0	0					Unique command

FIG. 26A

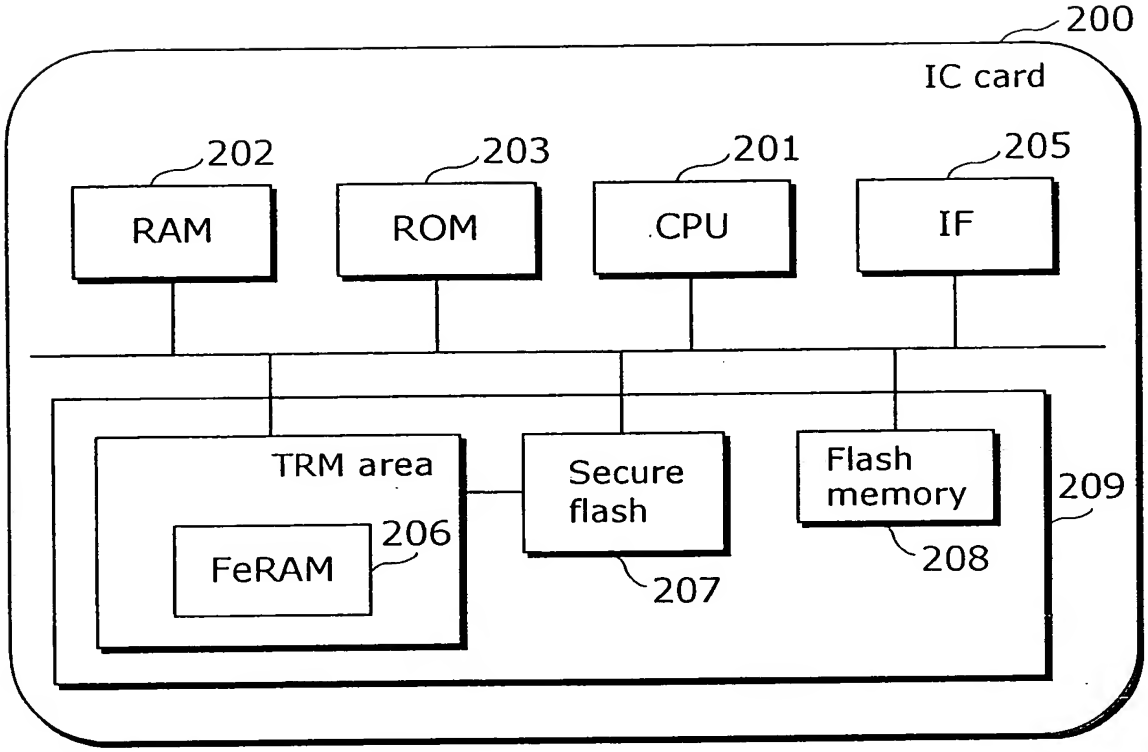


FIG. 26B